REMARKS

In response to the Office Action dated June 29, 2005, Applicant respectfully requests reconsideration and withdrawal of the rejections of the claims.

The Office Action requests that the Abstract, submitted with the Preliminary Amendment filed September 26, 2001, be presented on a separate sheet. In response thereto, a copy of the Abstract on a separate sheet is attached to this Amendment.

Claims 1, 3, 5, 7 and 9-12 were rejected under 35 U.S.C. § 102, on the grounds that they were considered to be anticipated by the publication of Lopez et al. entitled "Improved Algorithms for Elliptic Curve Arithmetic in GF (2^n)," identified in the Office Action as "Julio." Claims 2, 4, 6 and 8 were rejected under 35 U.S.C. § 103 on the basis of the Lopez et al. publication in view of the Solinas publication entitled "An Improved Algorithm for Arithmetic on a Family of Elliptic Curves." Claim 13 was rejected on the basis of the Lopez et al. publication and the Vanstone et al. patent. For the reasons presented below, it is respectfully submitted that the Lopez et al. publication does not anticipate, nor otherwise suggest, the subject matter of the pending claims.

The claimed invention is directed to a countermeasure method in a cryptographic system, to protect against the ability of unauthorized persons to discover a private

deciphering key, particularly for enciphering algorithms that employ elliptical curves. As explained in the background portion of the application, by monitoring the current consumption of a circuit that implements the cryptographic algorithm over a number of iterations, it becomes possible to determine the value of the bits that constitute a secret key. In accordance with the claimed subject matter, attacks of this type can be thwarted by making intermediate values of the calculations random, and therefore unpredictable. Pursuant to the invention, the calculations are made random by choosing a random representative of a point on the elliptic curve, on which the calculation is carried out. As recited in claim 1, for example, the counter measure method includes, as a first step, drawing at random an integer λ such that $0<\lambda<p$, where p is a prime number. Then, for a point P on the elliptical curve, a random representative P' of that point is calculated, by using the random integer λ.

It is respectfully submitted that the Lopez et al. publication does not disclose this claimed concept. In relevant part, in section 5 appearing on pages 7-9, it discloses the known use of projective coordinates to perform arithmetic operations on points on an elliptic curve. This known technique is described in the background portion of the present application, for example, beginning on page 4. The

Lopez et al publication does not disclose, however, the concept of choosing a random representative of a point on an elliptic curve, on which to perform a calculation. In apparent recognition of this difference, it is noted that the Office Action does not address this particular feature recited in the claims. In particular, it does not identify where the Lopez et al. publication discloses the first claimed step of "drawing at random an integer…." The rejection skips over this portion of the claim.

Upon review of the record, it was noted that typographical errors occurred in the presentation of the claims in the Preliminary Amendment filed September 26, 2001. Throughout the specification and the original claims, the randomly drawn integer is represented by the Greek character "lambda". Another random integer, recited in claim 4, for example, is represented by the Greek character "mu". It has been noted that the font that was employed for the Preliminary Amendment displayed the Greek character lambda as the letter "l", and the Greek character mu as the letter "m". Unfortunately, this transposition of characters was not caught before the Preliminary Amendment was filed.

To correct this typographical error in the claims, they are re-presented herein with the appropriate Greek characters for the randomly drawn integers, so that they conform to the

claims as originally presented. The changes to the claims do not constitute substantive amendments, but merely correct the characters employed to represent the random integers so that they are consistent with those appearing in the specification.

Upon review of the Office Action, it appears that the Examiner may have interpreted the symbol for the randomly drawn integer as the number "1", rather than the letter "l". It is respectfully submitted, however, that a person of ordinary skill in the art would not interpret the claim in such a manner. Specifically, if the same integer, i.e. 1, where to be drawn each time, it would not be considered to be a "random" drawing. Rather, it would be the selection of a predetermined value. That, of course, would be inconsistent with the objective of the invention, which is to randomize the representation of the point P on the elliptic curve upon which the calculation is based.

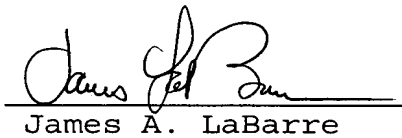
In summary, it is respectfully submitted that the Lopez et al. publication does not teach all of the steps recited in claim 1. Specifically, it does not disclose the steps of selecting a random integer, and using that integer to define the coordinates of a point P' that represents another point P on the elliptic curve. For at least this reason, therefore, the publication does not anticipate the subject matter of claim 1, nor any of the claims that depend therefrom.

Similarly, the Solinas publication does not disclose, nor otherwise suggest, this distinctive feature of the invention. This latter reference was relied upon in the Office Action as disclosing an algorithm to perform squaring, elliptic group operation, multiplication and addition-subtraction. Likewise, the Vanstone et al. patent applied, in the rejection of claim 13, does not disclose the use of a random representative of a point on an elliptic curve to perform cryptographic calculations. Rather, this reference was relied upon for its disclosure of a smart card, per se.

For the foregoing reasons, it is respectfully submitted that all pending claims are allowable over the prior art of record. Reconsideration and withdrawal of the rejections are respectfully requested.

Respectfully submitted,

BUCHANAN INGERSOLL PC

Date: September 29, 2005 By: 

James A. LaBarre
Registration No. 28,632

P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620